Ekwan E. Rhow (CA SBN 174604)
erhow@birdmarella.com
Marc E. Masters (CA SBN 208375)
mmasters@birdmarella.com
Christopher J. Lee (CA SBN 322140)
clee@birdmarella.com
BIRD, MARELLA, BOXER,
WOLPERT, NESSIM, DROOKS,
LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

Kalpana Srinivasan (CA SBN 237460)
Steven Sklaver (CA SBN 237612)
Michael Gervais (CA SBN 330731)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars
14th Floor
Los Angeles, CA 90067
Telephone: (310) 789-3100
ksrinivasan@susmangodfrey.com
ssklaver@susmangodfrey.com
mgervais@susmangodfrey.com

Jonathan M. Rotter (CA SBN 234137)
Kara M. Wolke (CA SBN 241521)
Gregory B. Linkh (*pro hac vice*)
GLANCY PRONGAY & MURRAY, LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
jrotter@glancylaw.com
kwolke@glancylaw.com
glinkh@glancylaw.com

Y. Gloria Park (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1301 Ave. of the Americas
32nd Floor
New York, NY 10019
Telephone: (212) 336-8330
gpark@susmangodfrey.com

Attorneys for Plaintiffs Bernadine Griffith, Patricia Shih, Rhonda Irvin, Matthew Rauch, and Jacob Watters

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, EASTERN DIVISION

BERNADINE GRIFFITH; PATRICIA SHIH; RHONDA IRVIN; MATTHEW RAUCH; and JACOB WATTERS, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

TIKTOK, INC, a corporation; BYTEDANCE, INC., a corporation,

Defendants.

CASE NO. 5:23-cv-00964-SB-E

PLAINTIFFS' OPPOSITION TO DEFENDANTS TIKTOK INC. AND BYTEDANCE INC.'S MOTION TO DISMISS FIRST AMENDED COMPLAINT

Date: December 15, 2023
Time: 8:30 a.m.
Crtrm.: 6C

Assigned to Hon. Stanley Blumenfeld, Jr.
Courtroom 6C

Action Filed: May 26, 2023
Trial Date: 9/30/2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

Federal Statutes

I. INTRODUCTION

The bulk of Defendants' Motion to Dismiss the First Amended Complaint ("FAC") is a belated motion for reconsideration of its prior motion to dismiss, which the Court largely denied. *See* Dkt. 59 ("Order"). Defendants rely on the same legal arguments the Court already rejected and ask the Court to dismiss claims it already upheld. Even the FAC's two new causes of action are based on the same conduct the Court already considered when it upheld most of Plaintiff's claims. In addition, the FAC addresses the Court's concerns with the two claims dismissed without prejudice by adding more factual allegations to support them. In response, Defendants merely re-litigate every cause of action previously upheld by the Court. The Court should deny the motion in its entirety.

<u>Privacy Claims</u>: Plaintiffs' allegations are sufficient to state a claim for invasion of privacy and intrusion upon seclusion. Defendants seek to relitigate the Court's prior holding by misinterpreting *In re Facebook, Inc. Internet Tracking Litig.* ("*Facebook Tracking*"), 956 F.3d 603 (9th Cir. 2020), and its straightforward holding that the surreptitious mass collection of full-string URLs violates a reasonable expectation of privacy. *Id.* at 605 (denying motion to dismiss where pleadings allege a reasonable expectation of privacy in "full-string detailed URLs" which contain "the name of a website, folder and sub-folders on the web-server, and the name of the precise file requested").

Defendants are incorrect in arguing Plaintiffs must plead an explicit misrepresentation. Defendants claim Plaintiffs do not allege reliance on any explicit misrepresentation by TikTok and that Plaintiffs cannot do so because they are not users of the TikTok app. This argument is unsupported by caselaw and ignores the Court's statement that "[i]t is plausible that an internet user who has avoided using TikTok because of privacy concerns might be just as alarmed to find that TikTok is collecting her browsing data as a Facebook user would be to discover that Facebook tracks her conduct when she is logged out." Order 8.

Contrary to Defendants' claim, Plaintiffs have Article III standing. Harms against privacy interests have "long been actionable at ***common law***." *Facebook Tracking*, 956 F.3d at 598 (all emphases throughout brief added unless otherwise noted). Defendants' reliance on *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021) is misplaced. *TransUnion* merely holds that violation of a statute conferring procedural rights does not necessarily create standing: the standing test is whether plaintiffs can point to "close historical or common-law analogue" for the asserted claim. *Id*. at 2204. Thus, violations of a *substantive* right to privacy remain actionable. *See Brown v. Google LLC*, 2023 WL 5029899, at *5 (N.D. Cal. Aug. 7, 2023) (applying *TransUnion*, allowing privacy claims, and rejecting argument "that privacy harms are never concrete where only anonymized data is collected"); *Mastel v. Miniclip SA*, 549 F.Supp.3d 1129, 1139 (E.D. Cal. 2021) (rejecting argument that *TransUnion* overruled *Facebook Tracking*'s standing analysis).

<u>CIPA and ECPA</u>: Plaintiffs sufficiently allege claims under the California Invasion of Privacy Act ("CIPA") and its federal counterpart, the Electronic Communications Privacy Act ("ECPA" or "Wiretap Act"). First, Plaintiffs have pled the Pixel collects full-string URLs, referrer URLs, and search queries (FAC ¶¶47-49, 52), all of which courts have recognized as "contents" under CIPA and ECPA. *In re Meta Pixel Healthcare Litig*., 647 F.Supp.3d 778, 795-96 (N.D. Cal. 2022) ("descriptive URLs" and "query strings"); *In re Google RTB Consumer Priv. Litig*., 606 F.Supp.3d 935, 949 (N.D. Cal. 2022) ("URL of the page where the impression will be shown" and "referrer URL that caused navigation to the current page"). Defendants also misapprehend the FAC's allegations that websites are unable to stop Defendants from collecting full-string URLs through the Pixel. FAC ¶¶47-49.

<u>CFAA</u>: In response to the Court's ruling that Griffith had not adequately pled a claim under the Computer Fraud and Abuse Act ("CFAA") because she is not a federal employee or contractor and thus collection of her data does not necessarily create a national security danger, the FAC adds numerous allegations about how

Defendants' mass data collection on ordinary Americans, not just federal employees, is a threat to public health and safety. FAC ¶¶28-37. As alleged, for example, "the more the Chinese government knows about the behaviors and opinions of ordinary Americans, the more effectively it can influence the behaviors and opinions of the American public as a whole." *Id.* ¶36. Indeed, the FAC cites numerous government officials who have sounded the alarm about the national security implications of Defendants' mass surveillance of ordinary Americans. Defendants ignore all of these allegations. Further, new Plaintiff Patricia Shih has access through her work to confidential state transportation systems that require Criminal Justice Information Services Level 4 certification to access. FAC ¶118.

Statutory Larceny and Conversion: Ignoring the Court's ruling, Defendants assert the data they collect through the TikTok SDK is not property and is instead "unidentifiable information that TikTok is not even able to associate with any person." Mot. 18-19. The Court already rejected this argument as a disputed point of fact that is contrary to the pleadings and cannot be the basis of a 12(b)(6) dismissal. Order 15. As the Court recognized, "Plaintiff's complaint contains several pages of allegations describing the value and marketability of internet user data, including the opportunities for internet users to directly sell or otherwise monetize information about their online activity." Order 15-16. The Court need not revisit its holding.

California Unfair Competition Law ("UCL"): In response to the Court's ruling that Plaintiffs pleaded the existence of a property interest but not the existence of economic loss of that property interest, *see* Order 19 n.7, the FAC adds allegations that three of the five named Plaintiffs previously marketed or sought to market their private data in focus groups and surveys that compensated them for their opinions. FAC ¶¶115, 124, 144. With the increase in mass data harvesting without compensation, precisely as Defendants do with the TikTok SDK, such focus groups and surveys have declined in prevalence. FAC ¶¶84-85. Indeed, because Defendants "make available extensive information about [their] consumer preferences and activity without compensating [them] in any way," the value of their private data and of their participation in paid focus groups and surveys has been diminished. FAC ¶¶115, 124, 144. With these allegations, Plaintiffs have sufficiently pled an economic loss of property interest due to Defendants' conduct. *See Brown*, 2023 WL 5029899, at *21.

Unjust Enrichment: California law recognizes an independent cause of action for unjust enrichment. *See ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016) ("To allege unjust enrichment as an independent cause of action, a plaintiff must show that the defendant received and unjustly retained a benefit at the plaintiff's expense."). The FAC sufficiently states such a claim. FAC ¶¶39-130, 115, 124, 130, 138, 144, 237-238.

II. PROCEDURAL BACKGROUND

Plaintiff Bernadine Griffith filed her initial complaint on May 26, 2023. On July 24, 2023, Defendants moved to dismiss. On October 6, 2023, the Court denied the motion to dismiss as to all but the CFAA and UCL claims and granted leave to amend. Order 19.

On October 20, 2023, Plaintiffs filed their FAC. In addition to Griffith, the FAC names four additional Plaintiffs: Shih, Irvin, Rauch, and Watters. Among them, Shih works as a consultant for the Florida Department of Transportation, and has access to that office's internal network and confidential information. FAC ¶118. The FAC also adds two new claims, an ECPA violation and unjust enrichment. In addition to the websites of Hulu, Etsy, and Build-a-Bear that Griffith personally visited, Plaintiffs allege that Defendants have intercepted and collected their private data from Rite Aid, Upwork, The Vitamin Shoppe, and Feeding America. *Id.* ¶¶110, 120, 128, 134, 135, 136, 142. In addition, the FAC makes several new substantive allegations relevant to the instant motion:

The TikTok Pixel's default settings: The TikTok Pixel by default tracks "PageView" events, which collects (among other things) referrer URLs and full-string URLs for every webpage visited. FAC ¶¶47-50. While PageView has always been a default setting, earlier versions of the Pixel gave websites the option to manually deselect the PageView option. *Id.* ¶48. At some point, Defendants eliminated that option, making full-string URLs a nonnegotiable, baseline field of data collected through the Pixel. *Id.* The collection of full-string URLs gives Defendants the ability to track private and personally identifiable information from website visitors, including non-TikTok users. *Id.* ¶51.

The TikTok SDK's threat to public health and safety: As confirmed by growing scrutiny and concern from government officials, TikTok's collection of data on ordinary Americans presents a threat to national security. FAC ¶¶26-37. Indeed, these officials have sounded the alarm that Defendants' collection and storage of data on ordinary Americans pose a threat to national security. *Id.*; *see id.* ¶28 (Senators highlighting how "even Americans who are not using the [TikTok] platform are at risk of having their information collected by TikTok" and how "the transmission to TikTok of non-user IP addresses, a unique ID number, and information about what an individual is doing on a site provides a deep understanding of those individuals' interests, behaviors, and other sensitive matters").

Economic injury caused by the TikTok SDK: The FAC adds allegations regarding the economic value of Plaintiffs' data and the specific ways in which they can monetize it. FAC ¶82. In addition, Plaintiffs Griffith, Shih, and Watters allege they have or have attempted to market their data by participating in customer surveys and focus groups that compensate them for their participation. FAC ¶¶115, 124, 144. However, due to the increasing trend toward mass data harvesting without compensation (such as through the TikTok SDK), traditional methods such as surveys have declined in prevalence. FAC ¶¶84-85.

III. LEGAL STANDARD

At this stage, the Court accepts well-pleaded factual allegations as true and "construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co*., 519 F.3d 1025, 1031 (9th Cir. 2008). Plaintiffs need allege only "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

On a motion to dismiss an amended complaint, a Court should address only "allegations not included in the initial complaint or when a defendant did not have a 'sufficient defense' to dismiss the initial complaint and the amended complaint presents 'changed events and available defenses.'" *Oddei v. Optum, Inc.*, No. 2:21-CV-03974-SB-MRW, 2021 WL 6103347, at *3 (C.D. Cal. Oct. 15, 2021) (citation omitted). "But where 'the allegations against a particular defendant in an amended complaint do not change,' courts have been more reluctant to entertain a defendant's Rule 12(b) motion to dismiss the amended complaint." *Id.* (citation omitted) (denying in part motion to dismiss where amended complaint did not present changed events or available defenses but "address[ed] the allegations in her first and third claims that this Court previously found to be insufficient to survive a motion to dismiss").

IV. ARGUMENT

A. Plaintiffs (Again) State Claims For Invasion Of Privacy And Intrusion Upon Seclusion.

A violation of privacy rights under California law requires two elements: (1) that Defendants intentionally intruded upon an area where Plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person. *Facebook Tracking*, 956 F.3d at 601. Defendants challenge the sufficiency of the privacy claim as to the first element only. Mot. 7. To determine whether a reasonable expectation of privacy exists, courts must analyze whether the conduct at issue constitutes a "violation of the law or social norms." *Facebook Tracking*, 956 F.3d at 601-02 (citation omitted). This assessment requires considering "a variety of factors, including the customs, practices, and circumstances surrounding a defendant's particular activities" to determine "whether a user would reasonably expect that [Defendants] would have access to the user's individual data." *Id.* at 602.

1. Plaintiffs Still Allege A Reasonable Expectation Of Privacy.

Facebook Tracking is "on point and provides the relevant legal standard." Order 6. "In an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data is untenable." *Facebook Tracking*, 956 F.3d at 599 (citation omitted). Defendants disregarded *Facebook Tracking* in their first motion to dismiss and continue to ignore its primary holding: that an allegation of surreptitious mass collection of referrer and full-string URLs is sufficient to allege a reasonable expectation of privacy at the pleading stage. 956 F.3d at 603. Instead, Defendants continue to advance the "untenable" position that nothing sensitive was taken, a proposition that ignores both *Facebook Tracking* and the Court's Order. *See* Order 8. Defendants' insistence to the contrary notwithstanding, the *Facebook Tracking* standard requires the Court not to focus exclusively on the ***nature*** of the data, but to also consider the ***method*** and ***amount*** of collection. 956 F.3d at 603.

Even considering only the ***nature*** of the data taken, the FAC sufficiently alleges such data is sensitive. Regardless of configuration, the TikTok Pixel ***always*** collects referrer URLs and full-string URLs from all website visitors. FAC ¶¶47, 49-50. *Facebook Tracking* recognized the sensitivity of data contained in detailed referrer and full-string URLs because it can contain "the name of a website, folder and sub-folders on the web-server, and the name of the precise file requested" and can also reveal the content of search queries. 956 F.3d at 605; *see Meta Pixel*, 647 F.Supp.3d at 795 ("Case law also supports plaintiffs' position that individuals maintain a reasonable expectation of privacy in detailed URLs."). Indeed, the FAC alleges that "the full-string URL reveals an incredible amount of private and personally identifiable information" and offers concrete examples of the type of information that is revealed. FAC ¶51.

The ***amount*** of collection of this sensitive data only exacerbates the privacy violations because when mass-harvested, full-string URLs allow Defendants to obtain "a comprehensive browsing history" for each individual. *Facebook Tracking*, 956 F.3d at 603. Defendants collect an enormous amount of this private data from "millions of Americans" through at least half a million non-TikTok websites and then aggregate it to assemble "digital dossiers" and comprehensive profiles of internet activity and preferences. *Id.* ¶¶55, 60, 66-67. *Facebook Tracking* was clear that mass collection of sensitive data such as detailed URLs violates a reasonable expectation of privacy, and subsequent cases have agreed. *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 630 (N.D. Cal. 2021); *Brown*, 2023 WL 5029899, at *20.

As for the ***method*** of collection, Defendants' conduct is ***even more violative*** of social norms than the conduct in *Facebook Tracking*. Here, the putative class is not TikTok users who were logged out of the TikTok App, but rather visitors to websites where the TikTok SDK is installed and who have "never been registered users of the TikTok app or held any TikTok accounts." FAC ¶217. As the Court already recognized, "an internet user who has avoided using TikTok because of privacy concerns might be just as alarmed to find that TikTok is collecting her browsing data as a Facebook user would be to discover that Facebook tracks her conduct when she is logged out." Order 8. Further, Defendants also violated reasonable expectations of privacy by engineering the TikTok SDK to bypass the "block third-party cookies" browser settings adopted by security-conscious users. *Id.* ¶¶57-58. This resembles the conduct in *Calhoun*, where plaintiffs successfully alleged a privacy claim by alleging that Google collected data while circumventing the "do not sync" browser setting on Google Chrome. 526 F.Supp.3d at 630.

Doe v. Meta Platforms, Inc., No. 22-cv-03580-WHO, 2023 WL 5837443 (N.D. Cal. Sept. 7, 2023), does not alter the *Facebook Tracking* standard. While that court dismissed a privacy claim because Plaintiffs had not identified "with specificity what, if any, private or particularly sensitive information about them Meta allegedly received," *id.* at *8, it did so while distinguishing *Facebook Tracking*. Specifically, the court noted that the *Meta Platforms* plaintiffs ***had not alleged the taking of "a full-string detailed URL***" like the *Facebook Tracking* plaintiffs did and the Plaintiffs do here. *Id.*; FAC ¶¶47, 49. Defendants' reliance on *Katz-Lacabe v. Oracle America*, No. 22-cv-04792, 2023 WL 2838118 (N.D. Cal. Apr. 6, 2023), is equally misplaced. Contrary to Defendants' assertion, *Katz-Lacabe* never required "allegations [that] plaintiffs actually provided [sensitive] information to websites" to survive a motion to dismiss. *See* Mot. 10. To the contrary, the court quoted extensively from *Facebook Tracking* and ***declined*** to dismiss the privacy claims, despite acknowledging that facts regarding the defendant's data collection and aggregation were "alleged generally." *Katz-Lacabe*, 2023 WL 2838118, at *7; *id.* at *8 ("determinations of the egregiousness of the privacy intrusion are not usually resolved at the pleading stage").[1]

2. Plaintiffs Need Not Plead An Explicit Misrepresentation.

Defendants also attempt to distinguish *Facebook Tracking* by manufacturing

[1] Defendants also include passing references to a laundry list of irrelevant cases. *Doe I v. Sutter Health*, No. 34-2019-00258072, 2020 WL 1331948 (Cal. Super. Ct. Jan. 29, 2020) (unreported California trial court minute order about a single website that relied on the district court decision that was later ***reversed*** by *Facebook Tracking*), *U.S. v. Forrester*, 512 F.3d 500 (9th Cir. 2008), and *Smith v. Facebook, Inc.*, 262 F.Supp.3d 943 (N.D. Cal. 2017), all pre-date *Facebook Tracking*. *Cook v. GameStop, Inc.*, No. 2:22-cv-1292, 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023), applies Pennsylvania law. *D'Angelo v. Penny Opco, LLC*, No. 23-cv-0981, 2023 WL 7006793 (S.D. Cal. Oct. 24, 2023), and *Massie v. Gen. Motors LLC*, No. 21-787-RGA, 2022 WL 534468 (D. Del. Feb. 17, 2022), involve the tracking of customer interactions from a single website, not mass collection of data from multiple websites. *Hammerling v. Google LLC* focused solely on whether the relevant data collection was "highly offensive," an allegation which Defendants do not challenge here. No. 21-cv-09004, 2022 WL 17365255, at *8 (N.D. Cal. Dec. 1, 2022).

a false pleading requirement, namely that Plaintiffs must allege an affirmative misrepresentation by Defendants that Plaintiffs relied upon. They further argue "Plaintiffs cannot reasonably base any subjective expectation of privacy based on anything TikTok said or did" because they are not TikTok users. Mot. 7-9 & n.2. This argument is unsupported by any authority whatsoever. While *Facebook Tracking* identified Facebook's misrepresentations to its users as one of several relevant factors, nothing in that decision says that an explicit misrepresentation is ***required*** to establish a reasonable expectation of privacy. To the contrary, *Facebook Tracking* makes it clear that the Court's analysis should consider all "circumstances surrounding a defendant's particular activities" that would violate the privacy expectations of a reasonable user. 956 F.3d at 601-02. And as the Court already noted, "an internet user who has avoided using TikTok because of privacy concerns might be just as alarmed to find that TikTok is collecting her browsing data as a Facebook user would be to discover that Facebook tracks her conduct when she is logged out." Order 8; *see* FAC ¶¶108, 117, 126, 132, 140 (Plaintiffs avoided using TikTok due to privacy concerns).

Making an explicit misrepresentation a prerequisite for violation of privacy laws would lead to absurd and dystopian results. According to the Defendants, so long as Defendants fastidiously avoided making any representation to non-users, they would be free to engage in any and all forms of invasive surveillance against non-users without risk of liability. In fact, they would be free to collect ***more*** data from non-TikTok user who expressly avoided using TikTok because of privacy and security concerns, than from TikTok users. This is not the law.

3. Plaintiffs Have Article III Standing To Bring Privacy Claims.

To establish Article III standing, a Plaintiff must allege a "concrete and particularized" harm. *Facebook Tracking*, 956 F.3d at 597. "Violations of the right to privacy have long been actionable at common law." *Id.* (citation omitted). Based on these principles, the *Facebook Tracking* court found the plaintiffs had alleged a concrete harm to their common law privacy interest by alleging Facebook had used their browsing history and personally identifiable information to compile detailed user profiles that would reveal their preferences and activities. *Id.* at 599. (While Defendants challenge standing only as to Plaintiffs' privacy claims under common law and the California Constitution, *Facebook Tracking* held that this standing analysis also applies to violations of CIPA and ECPA, as those statutes "codify a substantive right to privacy." 956 F.3d at 598.)

The same analysis applies here. As the Court has recognized, the FAC's allegations regarding data collection are materially indistinguishable from those in *Facebook Tracking*. Order 7-8. The FAC also contains numerous detailed allegations that the data collected is personally identifiable. *See* FAC ¶¶39 (TikTok SDK "can and does illicitly harvest private and personally identifiable data, such as the webpages visited by users, search queries, User IDs, User Agent, phone numbers, email addresses, IP addresses, and more"); 51 (describing ways in which full-string URL alone can disclose personally identifiable information); 67 ("Defendants are able to associate the information they obtain . . . with personally identifying information of non-TikTok users."). As Defendants acknowledge, two Plaintiffs specifically allege their personally identifiable information was taken. *Id.* ¶¶110, 128. Four Plaintiffs allege that they created accounts on or ordered products from certain websites, a process that would be impossible without providing information such as an email address or physical address. *Id.* ¶¶111-112, 120-121, 128, 142. Taken together, these allegations are sufficient to establish standing.

Defendants' arguments to the contrary are unpersuasive. First, Defendants rely on *Popa v. PSP Group, LLC*, No. 23-cv-0294-JLR, 2023 WL 7001456 (W.D. Wash. Oct. 24, 2023), to argue the *Facebook Tracking*'s standing analysis is no longer good law after *TransUnion*, 141 S. Ct. 2190, and that Plaintiffs must allege the taking of specific personally identifiable information to establish standing. Not so. *TransUnion* held only that legislative enactments do not obviate the "concrete harm" requirement for Article III standing. *Id. TransUnion* does ***not*** invalidate, and instead affirms, standing based on traditionally recognized harms under the common law and harms based on constitutional rights. In fact, *TransUnion* expressly assured that "[v]arious intangible harms can also be concrete," including "disclosure of private information, and intrusion upon seclusion." *Id.* at 2204.

Because *Facebook Tracking*'s standing analysis as to the privacy claims relied on traditional common law principles, and not standing created whole cloth by federal statute, 956 F.3d at 598, it remains good law after *TransUnion*. *See Mastel*, 549 F.Supp.3d at 1139 ("Though *Facebook Tracking* and *Eichenberger* were decided before *TransUnion*, they are not overruled by *TransUnion.*"); *Brown*, 2023 WL 5029899, at *5 (discussing *TransUnion* and rejecting argument that "privacy harms are never concrete where only anonymized data is collected").

Defendants' cases are easily distinguishable. *Popa*, 2023 WL 7001456, *Massie* 2022 WL 534468, and *Lightoller v. Jetblue Airways Corp.*, No. 23-CV-00361-H-KSC, 2023 WL 3963823 (S.D. Cal. June 12, 2023), are all Session Replay Code ("SRC") cases, which involve the tracking of consumer activity data on a single commercial website. *Massie* itself explicitly distinguishes these one-website SRC cases from *Facebook Tracking*, noting the degree of harm to privacy interests alleged in the former was "hardly comparable" to the latter. 2022 WL 534468, at *3. Finally, *Dinerstein v. Google, LLC*, 73 F.4th 502 (7th Cir. 2023), which deals with the dissemination of anonymized health records, not the mass collection of private data that Plaintiffs allege is personally identifiable, is inapposite.

B. Plaintiffs (Again) State A Claim Under CIPA And Adequately Allege An ECPA Claim.

1. Data Collected Through The TikTok SDK Is "Content" Under CIPA And ECPA.

ECPA defines the term "contents," when used with respect to electronic communication, to include "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). The Ninth Circuit held that "contents," under ECPA, means "the intended message conveyed by the communication," as opposed to "record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Privacy Litig.*, 750 F. 3d 1098, 1106 (9th Cir. 2014). "URLs are record information when they ***only*** reveal a general webpage address and basic identification information, ***but*** when they reproduce a person's personal search engine queries, they are contents." *Gershzon v. Meta Platforms, Inc.*, No. 23-cv-00083, 2023 WL 5420234, at *12 (N.D. Cal. Aug. 22, 2023) (citation omitted). "The analysis for a violation of CIPA is the same as that under the Federal Wiretap Act." *Brodsky v. Apple Inc.*, 445 F.Supp.3d 110, 127 (N.D. Cal. 2020).

Courts in this Circuit and beyond have found full-string URLs and search queries to constitute "contents" under ECPA and CIPA. *See, e.g.*, *Gershzon*, 2023 WL 5420234, at *13 (CIPA's "contents" requirement satisfied where "the Pixel transmits to Meta the URL of each page visited on a website"); *Meta Pixel*, 647 F.Supp.3d at 795 (descriptive URLs that "include both the 'path' and the 'query string'" are "contents" under ECPA); *Google RTB*, 606 F.Supp.3d at 949 (ECPA "contents" include "URL of the page where the impression will be shown" and "referrer URL that caused navigation to the current page"); *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 139 (3rd Cir. 2015) ("post-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user" is ECPA "contents"); *Brown*, 2023 WL 5029899, at *15-16 (search queries are "not like the 'outside of an envelope,' revealing the address and name of the recipient, but instead the contents of a letter").

The FAC alleges the TikTok SDK harvests, among other data, full-string URLs, "including the full document path with folder and subfolder structure" (FAC ¶49) and search queries (*id.* ¶¶39, 52, 55); *see id.* ¶¶168, 226 ("The communications intercepted by Defendants include 'contents' . . . in the form of detailed URL requests, webpage browsing histories and search queries, and URLs containing the specific search queries"); *id.* ¶¶109, 119, 133, 137, 141. Such data reveals substantive private content. *Id*. ¶51 ("For instance, the URL of a 'thank you' page to which a non-TikTok website visitor is directed after making a donation on a webpage could include private information like the visitor's email, country, amount of donation, and payment method.").

Defendants complain about a host of allegedly missing allegations, *see* Mot. 14, but they overlook the allegations that full-string URLs (that contain specific search queries and the full document path with folder and subfolder structure) are collected as "nonnegotiable, baseline data" from the half a million websites that have or had used the Pixel. FAC ¶¶51, 231. Further, contrary to Defendants' representations, Plaintiffs specifically alleged they "searched and browsed for" medication on Rite Aid, services and job offers on Upwork, television shows on Hulu, products on Etsy, health supplements on The Vitamin Shoppe, and volunteer opportunities on Feeding America. *Id.* ¶¶110, 121-122, 128, 134-136, 142.

Defendants' reliance on *Cook v. GameStop*, 2023 WL 5529772, is misplaced. *Cook* is another one-website SRC case, which alleged violations of the Pennsylvania Wiretap Act. *Id*. at *1. Unlike the complaint in *Cook* that lacked "critical necessary details for the Court's analysis of the type of information allegedly captured by GameStop's [SRC]," *id*. at *7, the FAC here details the specific minimum data fields captured by the TikTok SDK, *see* FAC ¶¶39, 49, 52, as well as the specific websites using the TikTok SDK visited by each Plaintiff. *Id*. ¶¶110-13, 120-22, 128, 134-36, 142. Further fatal to the *Cook* complaint was its allegations about how SRC works in general without any specific allegations about whether GameStop's code operated in that manner. 2023 WL 5529772, at *7. Here, by contrast, Plaintiffs not only alleged how pixels and cookies work in general but also alleged specific details about how the TikTok Pixel and Events API operate to circumvent browser cookie settings and intercept Plaintiffs' data. FAC ¶¶46-59.

2. Plaintiffs Allege An "Interception" Under CIPA.

Defendants repeat the already-rejected argument that they should avoid CIPA liability because they merely "provide[] a tool used by another." Mot. 15. Once again, "Defendants identify no authority suggesting that they cannot be held liable for eavesdropping because a third party, acting on Defendants' recommendation, participated in the installation of Defendants' code that sends information to Defendants." Order 11. In fact, courts in this Circuit have upheld CIPA claims concerning similar interception technology. For instance, in *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019), Moosejaw embedded software on its webpages that allowed third-party NaviStone to scan a user's computer. The court upheld claims against both defendants, finding the plaintiff "adequately alleges that NaviStone acted as a third party that eavesdropped on his communications with Moosejaw because the code embedded into the Moosejaw.com pages functioned as a wiretap that redirected his communications to NaviStone while he browsed the site." *Id*. at *1.

Defendants' assertion that the FAC's new allegations supply facts that websites "break the causal chain from Defendants' acts" have it entirely backward. The FAC's allegations confirm that Defendants' conduct goes beyond "recommend[ing] settings or encourag[ing] use of its Pixel." *See* Mot. 16. Indeed, Defendants have intentionally designed the TikTok Pixel so that it, ***by default***, tracks any "PageView event," which in turn transmits full-string URLs to Defendants. FAC ¶47. Defendants have intentionally "***provide[d] no way for websites to remove or deselect the tracking of PageView events***," which means that "***the collection of full-string URLs is a non-negotiable component of the TikTok Pixel***." *Id.* Even if a website chooses ***not*** to share search queries with Defendants by not configuring the Pixel to collect the Search event, FAC ¶52, Defendants collect search queries anyway by collecting them through the full-string URL, *id.* ¶231 ("full string URLS [] provide Defendants with the search terms of each user"), ¶168

("URLs containing the specific search queries"). Finally, the FAC alleges the default TikTok Pixel has become more invasive over time: certain earlier iterations of the Pixel gave websites the option to deselect the default PageView event, but the current version has eliminated this choice. *Id.* ¶48. Far from "websites' decisions break[ing] the causal chain from Defendants' acts," the websites have experienced ***decreasing*** agency in deciding what data is collected for Defendants' use and benefit.

Defendants' cases are inapposite. The court already distinguished *Lopez v. Apple*, 519 F.Supp.3d 672, 690 (N.D. Cal. 2021), Order 11, and Defendants have provided no additional analysis of the case now. *Liapes v. Facebook, Inc.*, 95 Cal.App. 5th 910, 923 (2023), concerned violations of the Unruh Civil Rights Act, not CIPA.

C. Plaintiffs Sufficiently Allege A Claim Under ECPA.

As Defendants note, "[t]he analysis for a violation of CIPA is the same as that under the federal Wiretap Act." Mot. 17 (quoting *Brodsky*, 445 F.Supp.3d at 127). Under Defendants' own logic, because Plaintiffs adequately allege CIPA claims, the ECPA claim should also survive.

Defendants specifically fail to address the issue of consent under ECPA even though they bear the burden of demonstrating consent. *Calhoun*, 526 F.Supp.3d at 620. They have thus waived any argument as to consent. *Zamani v. Carnes*, 491 F.3d 990, 997 (9th Cir. 2007) ("The district court need not consider arguments raised for the first time in a reply brief."); *FT Travel—New York, LLC v. Your Travel Ctr., Inc.*, 112 F.Supp.3d 1063, 1079 (C.D. Cal. 2015).

D. The FAC Sufficiently Alleges A CFAA Claim.

The Court previously found Griffith had not sufficiently pled that Defendants' conduct constituted a threat to public health and safety because "[s]he does not allege that she is a federal employe[e] or contractor, that the information gathered by TikTok may be used to blackmail her or commit corporate espionage, or that it threatens to cause physical or environmental harm." Order 14. In response, in addition to adding a plaintiff whose work requires a Criminal Justice Information Services Level 4 certification, FAC ¶118, the FAC adds numerous allegations concerning how Defendants' mass data collection regarding ordinary Americans—and not just federal employees or contractors—constitutes a threat to public health and safety. Numerous government officials have sounded the alarm that TikTok's uninhibited collection of data on ordinary Americans poses a national security risk. Yet Defendants ignore these new allegations.

The FAC quotes two U.S. Senators' letter to the Chair of the Committee on Foreign Investment in the United States expressing "'profound concern regarding the risks that TikTok poses to our ***national security*** . . .' given TikTok's ***collection of 'sensitive information of tens of millions of American users***.'" FAC ¶28. Critically, it goes on to quote the Senators' "profound concern" over TikTok's data collection about non-users that "provides a deep understanding of those individuals' interests, behaviors, and other sensitive matters" and that this data collection poses a threat to security. *Id.* According to a warning issued by the NSA Director, "control of the private data collected by TikTok" provides "a platform for information operations [and] a platform for surveillance" against the United States. *Id.* ¶31. "[T]he more the Chinese government knows about the behaviors and opinions of ordinary Americans, the more effectively it can influence the behaviors and opinions of the American public as a whole." *Id.* ¶36. Defendants' understanding of the behaviors and opinions of Americans is deepened and their influence is more effective because of their refusal to limit their data collection to TikTok app users only.

The FAC also recites an FCC Commissioner's effort to remove the TikTok app from Apple's and Google's app stores, citing how it "collects vast troves of sensitive data about those ***U.S. users***" and how "ByteDance officials in Beijing have repeatedly accessed the sensitive data that TikTok has collected ***from Americans***."

Id. ¶30. The FAC further notes the U.S. Senate's ongoing scrutiny over TikTok and how it "allowed private data about American users to be stored and accessed in China." *Id.* ¶33. In sum, the FAC sufficiently alleges how TikTok's collection of private data from ordinary Americans constitutes a threat to public health and safety.

Defendants' citation to *Sartori v. Schrodt*, 424 F.Supp.3d 1121 (N.D. Fla. 2019) is wholly distinguishable. *Sartori* involved a cheating ex-husband's allegation that his former wife violated the CFAA when she accessed his email account on their shared laptop for evidence of his extramarital affairs. The court found the husband had failed to show how his wife's "accessing his Gmail account *per se* led to increased divorce expenditures." *Id.* at 1129. Those facts couldn't be more different from those alleged here—that multinational corporations with ties to the Chinese government intercept data from millions of unwitting Americans notwithstanding state and federal government officials' growing concern over the national security implications of this surveillance.

Even if the Court disagrees that Defendants' conduct poses a threat to public health and safety when carried out against ordinary Americans, the FAC notes how the TikTok Pixel was found on "'more than two dozen' official websites of state governments" and how "[t]he presence of that code means that U.S. state governments around the country are inadvertently participating in a data-collection effort for a foreign-owned company, one that . . . could be harmful to U.S. national security and the privacy of Americans.'" FAC ¶65.

Finally, Defendants continue to concede "the placement of cookies on Plaintiff's computer can constitute a violation of the CFAA." Order 13 (quoting *In re Toys R Us, Inc., Priv. Litig.*, No. 00-cv-2746, 2001 WL 34517252, at *11 (N.D. Cal. Oct. 9, 2001)); *see Mortensen v. Bresnan Commc'n, L.L.C.*, No. CV 10-13-BLG-RFC, 2010 WL 5140454, at *6, *8 (D. Mont. Dec. 13, 2010).

E. Plaintiffs (Again) State Statutory Larceny And Conversion Claims.

The Court already found Griffith sufficiently alleged a property right to her data, noting "Plaintiff's complaint contains several pages of allegations describing the value and marketability of internet user data, including the opportunities for internet users to directly sell or otherwise monetize information about their online activity." Order 15-16. The FAC ***added*** to these already-sufficient allegations, providing yet additional examples of how "individual users like Plaintiffs herein can sell or monetize their own data." FAC ¶82 (adding allegations about Screenwise Panel, Brave, Loginhood, Killi, and Bigtoken).

Notwithstanding the Order and without any evolution in the applicable caselaw, Defendants challenge Plaintiffs' statutory larceny and conversion claims. Their argument should be rejected (again). While Defendants complain that Plaintiffs must have "exclusive possession or control" over their data for that data to constitute property, Defendants overlook the FAC's express allegation that "[u]nder the CCPA, ***personal data now encompasses the legal right to exclude others***, which is an essential element of individual property." FAC ¶89. Defendants attempt to exempt themselves from the CCPA by noting it applies only to "identifiable information" and that "[i]t cannot be used to control unidentifiable information that TikTok is not even able to associate with any person, let alone a non-TikTok user." Mot. 18-19. Of course, Plaintiffs dispute this assertion, which is contrary to the pleadings. *See* Order 15 (setting aside Defendants' assertion that non-user data is "valueless by-product" as disputed and "in any event is outside—and contrary to—the pleadings").

Defendants point to inapposite criminal and bankruptcy cases (and even a treaty about the moon!) and cases they previously cited as part of their first failed attempt to dismiss these claims. Mot. 17-18 (citing *United States v. Abouammo*, No. 19-cr-00621-EMC-1, 2022 WL 17584238 (N.D. Cal. Dec. 12, 2022); *Sutter Health*, 2020 WL 1331948; *United States v. Green*, 12 F. 4th 970 (9th Cir. 2021)). But these far-afield cases do not alter the Court's recognition that the "growing trend across courts" is "to recognize the lost property value of personal information." Order 15 (quoting *Calhoun*, 526 F.Supp.3d at 635). While Defendants argue the existence of value alone is not determinative of a property right,[2] they fail to address the FAC's strengthened allegations not only on the value of data but also on the numerous opportunities that internet users like Plaintiffs have to monetize their data. *See* FAC ¶82. Defendants also cite *Fraley v. Facebook, Inc*., 830 F.Supp.2d 785 (N.D. Cal. 2011), but the court there held that plaintiffs sufficiently pled an economic harm from Facebook's use of their names and likenesses. Further, like the *Fraley* plaintiffs, Plaintiffs here "do not merely cite abstract economic concepts in support of their theory of economic injury, but rather point to specific examples" of how the personal information intercepted by Defendants is valued in the marketplace. *Id.* at 799; FAC ¶¶82, 84-85.

F. The FAC Sufficiently Alleges A UCL Claim.

In response to the Order, the FAC adds allegations that Plaintiffs Griffith and Shih marketed their private data in the past by participating in focus groups and surveys that compensated them for their participation. FAC ¶¶115, 124. Plaintiff Watters previously signed up to participate in such surveys. FAC ¶144. As to all three Plaintiffs, because Defendants "make available extensive information about [their] consumer preferences and activity without compensating [them] in any way," the value of their private data and of their participation in focus groups and surveys has been diminished. FAC ¶¶115, 124, 144; *see* FAC ¶99 ("Defendants' improper interception, collection, and use of that Private Data means that Plaintiffs' and Class

[2] Defendants cite *In re Meza*, 465 B.R. 152 (Bankr. D. Ariz. 2012), to support this proposition. Even setting aside the fact that *Meza* (a case about whether a change of beneficiary on a life insurance policy constitutes a transfer of property) is irrelevant, Defendants' citation to it is misleading. The *Meza* court observed "the existence of value alone is not determinative ***of whether state law protects a sufficient bundle of rights to be deemed a property interest***." *Id.* at 155-56. Here, California law plainly accords such protection to Plaintiffs' data, as evinced in the passage of the CCPA. FAC ¶¶88-89.

and Subclass members' Private Data is less marketable").

With these allegations, the FAC sufficiently pleads "the existence of economic loss associated with the alleged property interest sufficient to support a UCL claim." Order 19 n.7. Indeed, Griffith and Shih have alleged not only that they ***intended*** to sell their data but also that they ***indeed have sold their data*** in the past and that their ability to do so in the future has been impeded by Defendants' conduct. *See* Order 17 (discussing UCL allegations that would survive 12(b)(6) dismissal). Plaintiffs' allegations are akin to those in *Brown*, where the court denied summary judgment on the UCL claim where "Plaintiffs have shown that there is a market for their browsing data and Google's alleged surreptitious collection of the data inhibited plaintiffs' ability to participate in that market." 2023 WL 5029899, at *21.

G. The FAC Sufficiently Alleges An Unjust Enrichment Claim.

In *Hartford Casualty Ins. Co. v. J.R. Mktg., L.L.C.*, the California Supreme Court found that unjust enrichment claims were not limited to quasi-contractual relationships and clarified that "a privity of relationship between the parties is not necessarily required." 61 Cal. 4th 988, 998 (2015). Subsequent Ninth Circuit cases have followed this approach in recognizing an independent cause of action for unjust enrichment. *Bruton v. Gerber Prods. Co.*, 703 Fed. Appx. 468, 470 (9th Cir. 2017) (citing *Hartford Casualty* and observing that "the California Supreme Court has clarified California law, allowing an independent claim for unjust enrichment to proceed in an insurance dispute"); *ESG*, 828 F.3d at 1038 (unjust enrichment "states a claim for relief as an independent cause of action ***or*** as a quasi-contract claim for restitution").

"To allege unjust enrichment as an independent cause of action, a plaintiff must show that the defendant received and unjustly retained a benefit at the plaintiff's expense." *Id*. The FAC pleads those elements. It alleges that Defendants intercepted and collected their private data including the specific technical mechanism by which Defendants have done so. FAC ¶39-71, 238. It also alleges that Defendants unjustly benefited from that data, by using it to improve their predictive algorithms and technology, at the expense of the diminishment in value of Plaintiff's private data. *Id.* ¶¶68, 72-103, 115, 124, 130, 138, 144.

V. CONCLUSION

For the foregoing reasons, the Court should deny Defendants' Motion to Dismiss in its entirety. If the Court disagrees, Plaintiffs request leave to amend.

DATED: November 20, 2023

Ekwan E. Rhow
Marc E. Masters
Christopher J. Lee
BIRD MARELLA BOXER WOLPERT
NESSIM DROOKS LINCENBERG & RHOW,
P.C.

Jonathan M. Rotter
Kara M. Wolke
Gregory B. Linkh
GLANCY PRONGAY & MURRAY, LLP

Kalpana Srinivasan
Steven Sklaver
Michael Gervais
Gloria Park
SUSMAN GODFREY L.L.P.

By: *\/s/ Ekwan E. Rhow*

Attorneys for Plaintiffs

CERTIFICATE OF COMPLIANCE

The undersigned counsel of record for Plaintiff Bernadine Griffith certifies that this brief contains 6,988 words, which complies with the word limit of L.R. 11-6.1.

DATED: November 20, 2023 By: *___/s/ Ekwan E. Rhow___*

Ekwan E. Rhow
Attorney for Plaintiffs